



A REPORT
TO THE
MONTANA
LEGISLATURE

INFORMATION SYSTEMS AUDIT

Photocopier Data Security

Department of Administration

MAY 2012

LEGISLATIVE AUDIT
DIVISION

12DP-01

**LEGISLATIVE AUDIT
COMMITTEE**

REPRESENTATIVES

RANDY BRODEHL
brodehl@centurytel.net

TOM BURNETT
Tburnetthd63@hotmail.com

VIRGINIA COURT
virginiacourt@yahoo.com

MARY McNALLY
mcnallyhd49@gmail.com

TRUDI SCHMIDT
trudischmidt@q.com

WAYNE STAHL, VICE CHAIR
wstahl@nemontel.net

SENATORS

DEBBY BARRETT
grt3177@smtel.com

GARY BRANAE
garybranae@gmail.com

TAYLOR BROWN
taylor@northernbroadcasting.com

CLIFF LARSEN
cliff@larsenusa.com

FREDRICK (ERIC) MOORE
mail@SenatorEricMoore.com

MITCH TROPILA, CHAIR
tropila@mt.net

MEMBERS SERVE UNTIL A
MEMBER'S LEGISLATIVE TERM
OF OFFICE ENDS OR UNTIL A
SUCCESSOR IS APPOINTED,
WHICHEVER OCCURS FIRST.

§5-13-202(2), MCA

FRAUD HOTLINE
(STATEWIDE)
1-800-222-4446
(IN HELENA)
444-4446

INFORMATION SYSTEMS AUDITS

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting, information technology, computer science, mathematics, political science, and communications.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

AUDIT STAFF

KENT RICE

DALE STOUT

Reports can be found in electronic format at:
<http://leg.mt.gov/audit>

LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Deborah F. Butler, Legal Counsel



Deputy Legislative Auditors
Cindy Jorgenson
Angie Grove

May 2012

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an Information Systems audit at selected state agencies to confirm controls ensure photocopier data security.

The Department of Administration is statutorily responsible for establishing and maintaining security standards and policy, and for providing training regarding security of data. We reviewed Department contracting for photocopiers, as well as agency processes for securing photocopier data and determined audited agencies have generally implemented security controls. However, data security could be improved through increased awareness and improved contractual language. We issued two recommendations to the department to improve contractual language and address awareness through use of state IT groups.

We wish to express our appreciation to the audited agencies and the Department of Administration for their cooperation and assistance.

Respectfully submitted,

/s/ Tori Hunthausen

Tori Hunthausen, CPA
Legislative Auditor

TABLE OF CONTENTS

Appointed and Administrative Officials	ii
Report Summary	S-1
CHAPTER I – INTRODUCTION	1
Introduction	1
Audit Objectives.....	1
Audit Scope and Methodology	1
Copier Controls in Place	2
CHAPTER II – PHOTOCOPIER DATA SECURITY	3
Introduction	3
Data Security During Use.....	3
Scanned Data	3
Data Storage.....	4
Copier Contract and Automated Data Removal.....	4
Data Security at Disposal.....	5
Copier Tracking	6
Increasing Awareness.....	6
DEPARTMENT RESPONSE	
Department of Administration	A-1

APPOINTED AND ADMINISTRATIVE OFFICIALS

**Department of
Administration**

Janet R. Kelly, Director

Sheryl Olson, Deputy Director

Marvin Eicholtz, Administrator, General Services Division



MONTANA LEGISLATIVE AUDIT DIVISION

INFORMATION SYSTEMS AUDIT

Photocopier Data Security

Department of Administration

MAY 2012

12DP-01

REPORT SUMMARY

Photocopiers can have hard drives just like computers, and thus may store sensitive and confidential data internally. If not properly controlled, there is potential for unauthorized access to this data. Although, we did not identify any data security breaches, there is a lack of awareness of data security controls.

Context

Photocopiers are standard equipment in many state offices. Copiers in today's office can be multi-function devices that not only copy, but also print, scan, fax, and email all types of office information, including sensitive and confidential data. Since the early 2000's, most digital copiers have a hard drive, just like a computer. For a copier with a hard drive, data is stored internally. If this data is not removed from the hard drive or the hard drive destroyed when a copier is removed from service, sensitive data may be released to unauthorized individuals. For example, a news story released in 2010 identified federal surplus copiers with sensitive data still stored on hard drives. State IT policy requires all electronic data storage devices to have all data removed so it cannot be recovered (sanitized) or physically destroyed prior to disposal. State IT policy further requires agencies to maintain documentation of the disposal of these devices.

other four copiers is accessible by anyone on the same network.

While reviewing Department of Administration contracts for completeness we identified areas for strengthening contract language. For 15 agency locations outside of Helena, individuals responsible for copiers at 8 were not aware of any policy regarding copier hard drive disposal and 5 believed copier vendors, not agencies, are responsible for hard drive disposal. Furthermore, of nine reviewed agencies, three do not track sanitized/disposed hard drives.

Overall, we did not identify any copier data security breaches but noted controls could be strengthened. We noted some agency personnel are not aware of, or following, state IT policy. Using existing IT groups would facilitate awareness of photocopier data security policy and controls.

Results

We reviewed settings on 31 copiers to identify where the data is stored and what data protections were in place. Of those, seven copiers stored data on internal hard drives. Three of these require a username and password for data access, while data on the

Recommendation Concurrence	
Concur	2
Partially Concur	0
Do Not Concur	0
Source: Agency audit response included in final report.	

For a complete copy of the report (12DP-01) or for further information, contact the Legislative Audit Division at 406-444-3122; e-mail to lad@mt.gov; or check the web site at <http://leg.mt.gov/audit>

Report Fraud, Waste, and Abuse to the Legislative Auditor's FRAUD HOTLINE

Call toll-free 1-800-222-4446, or e-mail lad@mt.gov.

Chapter I – Introduction

Introduction

Photocopiers (copiers) are standard equipment in many state offices. Copiers in today's office can be multi-function devices that not only copy, but also print, scan, fax, and email all types of office information, including sensitive and confidential data. Since the early 2000's, most digital copiers have a hard drive, just like a computer. If a copier does not have a hard drive, data is removed when the copier is powered off. However, for a copier with a hard drive, data is stored internally. A news story released in 2010 identified federal surplus copiers with sensitive data still stored on hard drives. As a result, we decided to conduct an audit to determine if state agencies are securing data on photocopiers.

Audit Objectives

The overall purpose of the audit was to confirm controls are in place to ensure data stored on copiers is secured. Initial audit work determined existing controls helped protect the security of data on copiers, so we ultimately established the following specific objectives for this audit:

1. Determine if networked copier data is reasonably protected from unauthorized access.
2. Determine if agencies are aware of and use copier settings to automatically remove data from hard drives.
3. Determine if agencies track copiers and hard drives according to state policy.

Audit Scope and Methodology

This audit focused on security through copier data management practices. Work included:

- ♦ Interviewing agency, contract, and vendor personnel.
- ♦ Reviewing contracts.
- ♦ Visiting agency offices across the state.
- ♦ Observing copier functionality, settings, and management.
- ♦ Reviewing agency compliance with state law and state IT policy.

Audit work was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office.

Although copiers are used by all agencies, our audit reviewed copier data management practices at a judgmentally selected sample of agencies based on size, potential sensitivity of agency data, copier types, and offices outside Helena. The number of photocopiers sampled also varied between agencies to meet different audit objective requirements.

Copier Controls in Place

Overall, we did not identify any copier data security breaches but noted controls could be strengthened. While agencies have copier data security controls in place, some personnel are not aware of, or following, related policy. The remainder of this report discusses our findings and recommendations to improve copier data security.

Chapter II – Photocopier Data Security

Introduction

Our original concern with photocopier (copier) data security was that data would remain on hard drives and when the copiers were disposed of, the data could be accessed by unauthorized individuals. Furthermore §2-15-114, MCA, requires each agency provide an adequate level of security for all data. Preliminary audit work helped reduce this concern through the identification of existing controls. One of the controls we identified was an improvement in technology. Some photocopiers now have the ability to automatically remove data stored on hard drives. However, photocopier settings must be adjusted to accomplish this. Photocopiers can also connect to networks, scan data, transfer data via email, and even store data on portable drives. For photocopiers with internal hard drives, data will remain on the hard drive until some method of removal occurs. Methods include automatic or manual data removal during use, and data removal or hard drive destruction upon disposal. As a result, our audit work focused on verifying agency use of photocopier data security settings. We will first discuss data security during use then highlight areas related to copier pool contracts and data storage.

Data Security During Use

One way state agencies can procure copiers is by leasing through a contract administered by the Department of Administration (DOA). To ensure copier data security is included at the agency level, we reviewed the DOA copier contract with the vendor and leasing agencies. Copiers procured through this “copier pool” currently have technology allowing for automated data removal. There are five main methods used to copy data: 1) copy, 2) print, 3) fax, 4) email, and 5) scan. For the first four methods, the technology of photocopiers allows the data on the hard drive to be erased upon completion of the process. In other words, once the copy is made, the data stored on the hard drive is erased because it is no longer needed. As mentioned, copier settings must be adjusted to accomplish this automatically. For the fifth method, scanning, the data is not automatically erased because it is still needed after processing.

Scanned Data

DOA’s copier pool devices are setup to automatically remove all data except when scanned. Because a scanned document needs to be stored until a user acts on it, the pool copiers, by default, allow scanned data to be stored on device hard drives until manually removed. However, there are settings on these copiers allowing scanned data to be automatically removed at specified intervals. Initial audit work noted some agencies leasing pool copiers were not aware scanned data was not automatically removed by default.

We performed further audit work to determine awareness of the scanned data default and availability of settings to force automatic removal of all stored data. We observed settings and hard drive contents for 13 leased copier pool devices. IT management at each leasing agency was aware of the ability to set pool copiers for automatic data removal. The settings for each copier were set to automatically remove data every 2-30 days. Furthermore, we did not observe data on any of the 13 hard drives.

Data Storage

Copiers store data in different locations including internal hard drives, network drives, portable drives, and email. Copier settings control where data is stored. For example, as noted above, scanned documents are saved to a copier's internal hard drive by default, but settings can be changed to force storage to agency network drives, portable drives plugged directly into the copier, or email. If a copier is connected to an agency network and stores data on its hard drive, it may be possible for anyone on that network to observe the stored information. This increases the risk of unauthorized viewing and use of sensitive or confidential data.

We reviewed settings on 31 pool and nonpool copiers to identify storage locations and data protections. Of those, seven copiers stored data on internal hard drives. Three of these require a username and password for data access, while data on the other four copiers is accessible by anyone on the same network, potentially allowing unauthorized access to data. For example, if personnel information were scanned on one of these copiers, anyone with access on the same network would generally be able to view the scanned file until it was manually removed. However, all four copiers had automated data removal set and no data was observed on the drives at the time of testing.

CONCLUSION

We conclude, while the agencies we reviewed were aware of settings to force automatic removal of all stored data, some agencies store data on copier hard drives potentially allowing unauthorized access to data. However, data was either protected by a required username/password or copiers were set to automatically remove stored data.

Copier Contract and Automated Data Removal

As previously noted, DOA procures copiers for lease by state agencies (copier pool). DOA's procurement is managed through a vendor contract which contains copier security requirements such as ability to automatically remove data. However, it does not contain any requirements for copier hard drive management if a copier stops

working prior to the contract's end. These requirements are key for ensuring the state, not the vendor, is able to manage any data in nonfunctional copiers. For example, if a copier stops working and must be replaced, there is no contract requirement to ensure state agencies are allowed to either remove data on the copier's hard drive or destroy the hard drive.

When an agency leases a copier from the copier pool, an agreement between DOA and the leasing agency is signed. This agreement describes copier functionality and costs as well as agency responsibilities. However, it does not note copier security options such as automatic removal of data or what process is to be followed if a copier malfunctions. Without this knowledge agencies may not know the copiers have a hard drive and are at risk for not removing data as required by state policy.

RECOMMENDATION #1

We recommend the Department of Administration update all photocopier pool contracts to contain security and hard drive management requirements.

Data Security at Disposal

State IT policy requires all electronic data storage devices to have all data removed so it cannot be recovered (sanitized) or physically destroyed prior to disposal. If this does not occur, data could be accessible to unauthorized users. State IT policy further requires agencies to maintain documentation of the disposal of these devices. According to DOA, the intent for tracking is to provide accountability if sensitive data were released through a nonsanitized or destroyed hard drive. This policy applies to photocopiers with hard drives.

Although §2-15-114, MCA, states agency directors are responsible for ensuring an adequate level of data security, generally the IT staff have day-to-day data security responsibility. When remote offices become involved, data security can trickle down to staff with little or no IT knowledge, resulting in data security policies not being enforced. For example, in remote offices administrative assistants may be responsible for a copier with a hard drive and not know if the copier has a hard drive or what data security policies are to be followed. To ensure all copier drives are managed in accordance with IT policy, we reviewed agency samples to determine awareness of and compliance with IT policy requirements.

Copier Tracking

We reviewed 15 locations outside of Helena for IT policy awareness. Individuals responsible for copiers at eight were not aware of any policy regarding copier hard drive disposal and five believed copier vendors, not agencies, are responsible for hard drive disposal. As a result, risk is higher at office locations outside Helena because copier hard drives with sensitive data could be accessible to unauthorized users.

We then reviewed agency procedures for copier hard drive tracking when devices are sanitized or destroyed. We noted the following:

- ♦ Three agencies track copier hard drive disposal.
- ♦ Two agencies have not disposed of any copier hard drives but indicated state policy would be followed.
- ♦ One agency stated tracking sanitized or destroyed hard drives occurs through help desk software; however, they could not supply us with any examples to support their statement. As a result, we could not determine if the agency tracks hard drive sanitation and destruction.
- ♦ Three agencies do not track copier hard drive sanitizing or destruction.

Agency personnel responsible for copier management noted multiple reasons for not tracking copier hard drives. The most common was unawareness of the tracking requirement and that all sanitized/destroyed drives are to be tracked, regardless of disposal methods or reasons for disposal. Smaller agencies stated since they only have a limited number of copiers, there is no need to track them because they can remember them all. However, if agency personnel change, this knowledge could be lost. Documenting hard drive disposal, as required, would prevent loss of information.

Increasing Awareness

We originally had concerns over the security of data on photocopiers. Upon completion of audit work to verify measures taken to secure data, we determined our initial concerns were reduced due to identification of existing controls. While we did not identify any data breaches during our audit, we believe controls can be strengthened by increasing the awareness of existing policies and need for securing data on photocopiers. Additionally, while we only included a sample of agencies in our audit, photocopier data security requirements apply to all state agencies.

State law (§2-17-534, MCA) places responsibility for providing security standards and policies with the Department of Administration. The law also requires the department to provide for a training program regarding security of data. A potential method of educating all staff managing copiers is to instruct agency IT management of the data security policy while reiterating the importance of the knowledge trickling down to

all levels of copier managers, including those in remote offices. The state has agency IT management level groups (Information Technology Board, Network Managers Group, Information Technology Managers Committee, etc.) to keep agency staff aware of, and manage, IT issues. Increasing awareness of state IT policy expectations, including tracking of all sanitized/destroyed hard drives, would help ensure agencies meet all aspects of policy.

RECOMMENDATION #2

We recommend the Department of Administration use existing Information Technology groups to facilitate awareness of state data security policy.

DEPARTMENT OF
ADMINISTRATION

DEPARTMENT RESPONSE

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

A-1



BRIAN SCHWEITZER, GOVERNOR

JANET R. KELLY, DIRECTOR

STATE OF MONTANA

(406) 444-2032
FAX (406) 444-6194

MITCHELL BUILDING
125 N. ROBERTS, RM 155
PO BOX 200101
HELENA, MONTANA 59620-0101

May 21, 2012

RECEIVED

MAY 21 2012

LEGISLATIVE AUDIT DIV.

Ms. Tori Hunthausen, CPA
Legislative Auditor
Legislative Audit Division
PO Box 201705
Helena, MT 59620-1705

RE: Information Systems Audit #12DP-01: Photocopier Data Security

Dear Ms. Hunthausen:

The Department of Administration has reviewed Audit #12DP-01: Photocopier Data Security. The Department's responses to the recommendations are below.

Recommendation #1

We recommend the Department of Administration update all photocopier pool contracts to contain security and hard drive management requirements.

Response: Concur.

The Department will amend all photocopier pool contracts to ensure agencies properly configure photocopiers to automatically remove data from hard drives at the time of use. Further, photocopier pool contracts will specify that data must be erased or the hard drive removed when a photocopier is replaced.

Recommendation #2

We recommend that the Department of Administration use existing IT Groups to facilitate awareness of state data security policy.

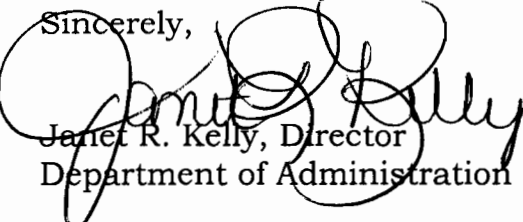
Response: Concur.

The Department will continue to use the Information Security Managers Group, the Information Technology Managers Council, and the Information Technology Board to facilitate awareness of state data security policy. In addition, the Department will continue to use the Information Security Managers Group at its quarterly workshops and the annual Information Technology Conference to increase information security awareness, including media storage issues.

We appreciated the hard work and careful examination that you and your staff provided during this audit. Our department always looks upon the audit process as an opportunity to improve our operations and performance.

The Department's Corrective Action Plan (CAP) is enclosed.

Sincerely,



Janet R. Kelly, Director
Department of Administration

Enclosure

Preliminary Response
Corrective Action Plan: Audit Report #12DP-01
Photocopier Data Security
Department of Administration
May 21, 2012

Agency	Recommendation #	Does this affect a federal program?	CFDA # (if previous YES)	Management View	CAP – Corrective Action Plan	Person responsible for CAP	Target Date
61010	Recommendation # 1 We recommend the Department of Administration update all photocopier pool contracts to contain security and hard drive management requirements.	No		Concur	The Department will amend all photocopier pool contracts to ensure agencies properly configure photocopiers to automatically remove data from hard drives at the time of use. Further, photocopier pool contracts will specify that data must be erased or the hard drive removed when a photocopier is replaced.	Marvin Eicholtz	8/31/12
61010	Recommendation # 2 We recommend that the Department of Administration use existing IT Groups to facilitate awareness of state data security policy.	No		Concur	The Department will continue to use the Information Security Managers Group, the Information Technology Managers Council, and the Information Technology Board to facilitate awareness of state data security policy. In addition, the Department will continue to use the Information Security Managers Group at its quarterly workshops and the annual Information Technology Conference to increase information security awareness, including media storage issues.	Tammy LaVigne	Ongoing First iteration completed by 12/12